Erkenntnisse aus dem feministischen DSA-Plattform-Monitoring

Plattformregulierung muss Gewaltschutz priorisieren

Ein Policy Paper des bff

Bundesverband
Frauenberatungsstellen
und Frauennotrufe

bff Plattform-Monitoring mit Fokus auf Art. 12, 16, 34 und 35 DSA

Plattformregulierung muss Gewaltschutz priorisieren

Der *Digital Services Act (DSA)* ist das zentrale europäische Gesetz zur Regulierung großer Online-Plattformen. Sein Ziel ist es, digitale Räume sicherer zu machen, Grundrechte zu schützen und systemische Risiken wie Hass, Desinformation und geschlechtsspezifische Gewalt zu reduzieren. Für Betroffene von *(digitaler) geschlechtsspezifischer Gewalt* — etwa nicht-einvernehmlicher Verbreitung intimer Bilder (non-consensual intimate images, NCII), Deepfakes, Stalking oder Doxing – kann ein einziger Klick enorme, teils lebensverändernde Folgen haben. Plattformen spielen dabei eine zentrale Rolle: Sie entscheiden, was sichtbar wird, wie Inhalte verbreitet werden und wie Betroffene unterstützt werden.

Der DSA verpflichtet sehr große Online-Plattformen (*VLOPs*) und Suchmaschinen (*VLOSEs*) erstmals dazu, systemische Risiken aktiv zu erkennen und zu mindern, benutzer*innenfreundliche Meldewege bereitzustellen und zentrale Kontaktstellen für Betroffene einzurichten. Unser Monitoring zeigt jedoch: Trotz starker Rechtsgrundlagen scheitert die Umsetzung in der Praxis häufig – mit gravierenden Folgen für Betroffene.

Dieses Policy Paper zeigt,

- welche Pflichten besonders für Betroffene von geschlechtsspezifischer Gewalt relevant sind
- wo Plattformen versagen
- und welche feministischen, praxisorientierten politischen Maßnahmen jetzt nötig sind, um den Schutz vor (digitaler) geschlechtsspezifischer Gewalt zu gewährleisten

Grundlage unserer Analyse sind die systemischen Risikoberichte gemäß Artikel 34 DSA aus dem Jahr 2023, die wir von den großen sozialen Plattformen (Snapchat, TikTok, Instagram, Facebook) sowie bei Pornoplattformen (XVideos, Pornhub und Stripchat) ausgewertet haben.

Wichtige Artikel im Überblick

Art. 34 DSA – Risikoanalyse	VLOPs und VLOSEs müssen systemische Risiken – darunter explizit Risiken geschlechtsspezifischer Gewalt - regelmäßig identifizieren und bewerten.
Art. 35 DSA – Maßnahmen zur Risikominderung	Basierend auf den Risikoanalysen müssen wirksame Maßnahmen umgesetzt und deren Wirksamkeit kontinuierlich überprüft werden (z. B. sichere Meldewege, Moderation, algorithmische Anpassungen, Kooperation mit Expert*innen).
Art. 12 DSA – Kontaktstellen (SPOC)	Plattformen müssen eine zentrale, leicht auffindbare Kontaktstelle (SPOC) einrichten über die Betroffene und Beratungsstellen direkt kommunizieren können.
Art. 16 DSA – Leicht zugängliche Meldewege	Plattformen sind verpflichtet, benutzer*innenfreundliche und leicht zugängliche Meldewege bereitzustellen.

Wo hakt es in der Praxis?

Defizite bei Art. 34/35 – Risikoanalysen & Risikominderung

1. **Enge oder fehlende Definitionen von geschlechtsspezifischer Gewalt**
   Viele Plattformen definieren geschlechtsspezifische Gewalt zu eng und meist ohne intersektionale Perspektive. Diskriminierungen entlang von Geschlecht, Race, Klasse, Behinderung, Sexualität oder Migration werden kaum zusammen gedacht – obwohl genau diese Verschränkungen bestimmen, wie stark Menschen online von geschlechtsspezifischer Gewalt gefährdet sind. Außerdem erkennen viele Plattformen zentrale Formen geschlechtsspezifischer digitaler Gewalt, wie beispielsweise *Doxing* oder sexualisierte *Deepfakes*, nicht als solche an. Diese Angriffe werden häufig im sozialen Nahraum verübt – etwa durch (Ex-)Partner, Familienmitglieder oder Personen aus dem Umfeld – werden aber in Risikoberichten nicht als geschlechtsspezifische Gewalt eingeordnet.

2. **Mangelnde Verknüpfung zu realen Gewaltkontexten**
   Geschlechtsspezifische Gewalt wird als rein digitales Phänomen betrachtet. Digitale Gewalt als Fortsetzung von (Ex-)Partnerschaftsgewalt, psychischer Gewalt, Kontrolle und Überwachung in der analogen Welt bleibt von den Plattformen unberücksichtigt, obwohl diese Formen eng miteinander verwoben sind.

3. **Oberflächliche Risikoanalysen**
   Um Nutzer*innen besser vor illegalen Inhalten zu schützen, haben viele Plattformen zwar Maßnahmen wie Blockieren, Melden oder KI-Filter benannt, allerdings bleibt deren Effektivität und Zielgruppenbezug unklar. Geschäftsmodelle, die Risiken durch Werbung und Engagement- Optimierung erzeugen, werden kaum reflektiert. Viele Berichte wirken wie eine reine „Show Compliance“ ohne tiefgehende Analyse.

4. **Mangelnde Transparenz**
   Berichte sind uneinheitlich in Kategorien, Zeiträumen und Formaten eingeteilt/unterteilt, oft schwer auffindbar oder stellenweise sogar geschwärzt (z.B. TikTok). Snapchat stuft sexualisierte Gewalt, entgegen Studien[1], als „extrem niedriges Risiko“ ein. Fehlende Standards erschweren Vergleichbarkeit und externe Kontrolle.

5. **Werbung als unterschätztes Risiko**
   Über Monate wurden *Deepfake*-/*Nudify*-Apps über Meta Ads beworben[2] – teils auch für minderjährige Nutzer*innen sichtbar, die die Tragweite solcher Tools kaum einschätzen können. Gleichzeitig spielt auch Google Ads weiterhin Werbung für *Stalkerware*[3] aus. Werbung wird von Plattformen kaum als eigenständiges Risiko für geschlechtsspezifische Gewalt anerkannt, obwohl sie Gewalt befördert.

1 Snapchat, The Digital Well-Being Index – Key Research Results, February 2023: https://assets.ctfassets.net/kw9k15zxztrs/f8tyHpE9HzLT9bGpPIg9B/e92cf6506b284bf4d27f0fef6bb1e264/DWBI_Findings_English.pdf
2 Quelle: 404 Media, 15.01.2025, „Instagram Ads send this nudify Site 90 Percent of its traffic”, https://www.404media.co/instagram-ads-send-this-nudify-site-90-percent-of-its-traffic/
3 Quelle; August 2024, Complaint against Google Ireland Limited regarding Art. 35 (1) in conjunction with Art. 34 (1) DSA, submitted by Gesellschaft für Freiheitsrechte e.V. in cooperation with the project “Ein Team gegen digitale Gewalt“, https://freiheitsrechte.org/uploads/documents/Englische-Dokumente/Freedom-in-the-digital-Age/Complaint-Google-Stalking-Apps.pdf

Empfehlungen zu Art. 34/35 DSA

- Harmonisierung der Risikoanalysen durch Mindeststandards für Kategorien, Zeiträume und Methodik
- Einrichtung eines permanenten, öffentlichen und maschinenlesbaren Archivs für alle DSA-Dokumente zur besseren Transparenz und Vergleichbarkeit
- Plattformen müssen geschlechtsspezifische Gewalt als Menschenrechtsverletzung anerkennen und dies in ihren Risikoanalysen sichtbar machen
- Entwicklung und verbindliche Umsetzung eines gemeinsamen, intersektionalen Gewaltverständnisses auf Basis der Istanbul-Konvention
- Durchführung ganzheitlicher Risikoanalysen, die technische, soziale und strukturelle Gewaltfaktoren verbinden
- Geschlechtsspezifische Gewalt ist kein Einzelrisiko, sondern wirkt systemisch über Moderation, Werbung, algorithmische Amplifizierung und Designentscheidungen hinweg. Risikoanalysen müssen diesen Querschnittscharakter verpflichtend abbilden
- Maßnahmen zur Risikominderung müssen ausdrücklich gender-sensibel und intersektional konzipiert sein, um erhöhte Risiken für unterschiedliche Betroffenengruppen anzuerkennen
- Plattformen müssen zivilgesellschaftliche Organisationen und Betroffene systematisch und vergütet in die Ausarbeitung ihrer Risikoberichte einbeziehen
- Einführung regulierter Standards zur Wirksamkeit, Zielgruppenorientierung und Evaluation von Risiko-Minderungsmaßnahmen
- Plattformen müssen offenlegen, welche Daten sie erheben und nutzen, sowie Maßnahmen systematisch nach Zielgruppen, Wirksamkeit und der spezifischen Vulnerabilität unterschiedlicher Gruppen evaluieren und veröffentlichen
- Klare Anerkennung von sexualisierten Deepfakes als geschlechtsspezifische Gewalt
- Einbeziehung der Bewerbung und Verbreitung von Programmen, die uneinvernehmliche sexualisierte Deepfakes ermöglichen, als eigenständigen Risikofaktor geschlechtsspezifischer Gewalt
- Plattformen sind bereits zur aktiven Risikominderung verpflichtet; diese Verpflichtung muss jedoch konsequent umgesetzt werden, insbesondere durch die systematische Entfernung von Werbung für entsprechende Anwendungen

Defizite bei Art. 12 – Kontaktstellen (SPOC)

1. **Schwer auffindbare Kontaktstellen:** SPOCs sind oft tief im Menü versteckt und nur über mehrere Klicks schwer erreichbar.
2. **Manipulative Oberflächen-Gestaltung:** Endlosscrollen oder kleinere Footer machen die Kontaktstelle praktisch unsichtbar.
3. **Sprachliche Barrieren** Viele SPOCs gibt es nur in Englisch oder juristisch komplizierter Sprache.
4. **Fehlende Betroffenenorientierung** Statt konkreter Ansprechpartner*innen finden Betroffene oft nur unklare Formulare oder FAQ-Seiten.
5. **Uneinheitliche und verwirrende Formulare** Es fehlt bei vielen Plattformen eine transparente Erklärung, was eine SPOC- oder DSA-Beschwerde ist und welche Rechte Betroffene haben.

Empfehlungen zu Art. 12 DSA

- SPOCs klar und gut sichtbar im Header oder Hauptmenü platzieren
- Direkter, manipulationsfreier Zugang ohne versteckte Klickpfade gewährleisten
- Einfache, barrierearme Sprache und automatische Sprachauswahl anbieten
- Verweis auf spezialisierte Hilfe (z.B. die Hilfsdatenbank des bff) integrieren
- Transparente Erklärung der Funktion der SPOCs und Rechte der Nutzenden aus dem DSA (Meldung, Beschwerde, Zugang zu *Trusted Flagger*/ *Außergerichtlichen Streitbeilegungsstellen*)

Defizite bei Art. 16 – Meldesysteme

Die stärksten Probleme liegen im Herzen des DSA: den Meldewegen selbst.
Zitat von Peer-Expert*in
Patricia Gutsche aus dem bff:

> „Ich fühle mich grundsätzlich bestärkt, wenn ich online etwas melden kann. Nur müssten die Meldewege viel einfacher sein, damit ich sie auch wirklich nutzen kann."

Die im Oktober 2025 von Das NETTZ veröffentlichte Studie zur Umsetzung der DSA-Meldewege auf großen Plattformen ist eine der ersten DSA-Untersuchungen, die zeigt, wie weit Gesetzesvorgaben und praktische Nutzbarkeit auseinanderliegen. Die Studie zeigt, dass die von der EU vorgesehen DSA-Meldewege schwer auffindbar und unklar gestaltet sind und deshalb kaum genutzt werden. Stattdessen melden Betroffene überwiegend über die herkömmlichen Meldewege Verstöße gegen die AGBs, die zwar einfacher wirken, aber nicht denselben rechtlichen Schutz bieten. Rund ein Viertel der DSA-Meldungen werden vorzeitig abgebrochen – ein Hinweis auf erhebliche Nutzungsbarrieren. Viele Betroffen wissen zudem nicht, dass der DSA ihnen spezielle Rechte einräumt, wodurch schwerwiegende Inhalte oft nicht über den korrekten Weg gemeldet werden. Die Folge ist eine strukturelle Unterausnutzung zentraler Schutzmechanismen des DSA.[1]

1. Unklare Kategorien
Betroffene müssen zwischen Strafrechtsbegriffen wählen, die sie nicht verstehen. Auf Snapchat ist für die Nutzer*innen nicht ersichtlich, ob sie gerade eine Meldung nach DSA oder wegen eines Verstoßes gegen die AGBs einreichen.

2. Manipulative Muster *(Deceptive Patterns)*
Plattformen lenken Betroffene bewusst weg von den DSA-Meldewegen und hin zu schwächeren AGB-Meldungen. Die Meldewege selbst enthalten Deceptive Patterns, wie irreführende Kategorien, die wie rechtliche Optionen wirken, aber keine DSA-Beschwerde auslösen oder verlängerte Klickpfade mit wiederholten Bestätigungen, die zu einer „*click fatigue*" führen.

3. Hohe Zugangshürden
Anforderungen wie Kontoerstellung, Adresspflicht oder Identitätsnachweise schließen vulnerable Gruppen aus, z.B. Personen mit unsicherem Aufenthaltsstatus. Außerdem erzeugen viele der Melde-Formulare den Eindruck eine offizielle Anzeige zu erstatten, bzw. einer Haftbarkeit der Nutzer*in für eine Falsch-Meldung.

4. Kein menschlicher Kontakt
Meldungen landen oft direkt in automatisierten Systemen. KI erkennt *NCII*, Deepfakes, Stalking und Abhängigkeitsverhältnisse kaum zuverlässig – selbst für Fachpersonen sind solche Fälle komplex. Zudem ist unklar, mit welchen Daten die Modelle trainiert werden. TikTok scheint beispielsweise auf automatisierte Moderation zu setzen, ohne dass dieser Umstand

1 Quelle: Das NETTZ, Studie: „Zwischen Klick und Konsequenz: Eine Evaluation der Meldeverfahren nach dem Digital Services Act", Oktober 2025, https://www.das-nettz.de/neue-studie-von-das-nettz-zeigt-durch-den-dsa-vorgegebene-meldeverfahren-auf-grossen-online

den Nutzer*innen transparent gemacht wird. Eine solche nicht gekennzeichnete automatisierte Entscheidung ist ein klarer Verstoß gegen Artikel 16 und 20 DSA[2]. Für Betroffene digitaler Gewalt fehlen damit menschliche, kontextsensible Bewertungen – oft genau das, was sie dringend brauchen.

5. Reviktimisierende Prozesse
Fehlende Erklärungen, algorithmische Fehlentscheidungen und automatisierte Ablehnungen verstärken Scham, Ohnmacht und Verzweiflung bei den Betroffenen.

6. Fehlende sprachliche Zugänglichkeit
Junge Menschen, Menschen mit Lernschwierigkeiten und nicht-Muttersprachler*innen sind besonders gefährdet, die Meldewege gar nicht erst zu finden oder sind für diese Gruppen nicht nutzbar.

2 Quelle: 2025, HateAid, „Recht ohne Reichweite – Der DSA im Praxistest“, https://www.stiftung-mercator.de/de/publikationen/hateaid-abschlussbericht-recht-ohne-reichweite/

bff-Empfehlungen zu Art. 16 DSA – Feministische Gestaltung von Meldewegen

*Diese Empfehlungen wurden im Rahmen des Digital Futures Gathering am 1./2. Oktober 2025 in Berlin kollaborativ in einem Workshop unter Leitung des bff mit dem Titel „Reporting Futures" gemeinsam mit internationalen Expert*innen aus Netzpolitik und Betroffenenberatung entwickelt.*

Zugang erleichtern

- Verbindliche EU-Leitlinien zur Bedeutung von einfach zugänglich und benutzer*innenfreundlich im Sinne des Art. 16 DSA definieren – inklusive klarer Mindeststandards zu Sprache, Navigation, Barrierefreiheit und transparenter Begriffserklärung
- Einheitlicher, sichtbarer Melde-Button auf allen Plattformen
- 2–3 klar verständliche Kategorien (z.B. bildbasierte Gewalt, Stalking, Doxing)
- Einfache, barrierearme Sprache mit Symbolen und Audiofunktion
- Keine riskanten Pflichtfelder (Adresse, Personalausweis-Nummer)
- Mehrere Zugangswege und Aufklärung darüber (Web, Chat, Telefon, Trusted Flaggers)

Schutz gewährleisten

- Trauma-informierte Bestätigungen und Erklärungen des Prozesses, die Betroffene nicht retraumatisieren
- Angemessene Ausstattung der nationalen *DSCs* und Aufklärungs-Kampagne durch sie
- Menschliche Prüfung statt rein automatisierter Moderation
- Sofortmaßnahmen bei hochriskanten Inhalten
- Garantien zum Datenschutz
- Sanktionen für manipulativen Muster oder systematisch fehlerhaften Meldewegen durch EU-Kommission und nationale Behörden

Betroffene beteiligen

- Co-Gestaltung der Meldewege mit Betroffenen und Expert*innen für Gewalt und digitale Zugänglichkeit
- Geschulte menschliche Inhalte-Moderator*innen (fair vergütet, Zugang zu Supervision, Schulung durch Gewaltschutz-Expert*innen)
- Eine europäische Meldestelle für NCII/Deepfakes, die mit bestehenden nationalen Meldestellen, Plattformen und Behörden vernetzt ist und Meldungen system- und plattformübergreifend bearbeiten kann (interoperabel)
- Transparente Schlüsselindikatoren aus Betroffenenperspektive (z. B. durchschnittliche Antwortzeit, Meldungen, die fälschlicherweise abgelehnt wurden, Anzahl der Klicks, die Nutzer*innen benötigen, um zum Meldeformular zu gelangen, Abbruchrate etc.)

Fazit

Die vorliegenden Analysen machen deutlich:
Geschlechtsspezifische (digitale) Gewalt ist kein Randphänomen, sondern ein strukturelles Problem, das durch die bestehenden Melde- und Beschwerdewege der Plattformen nicht ausreichend adressiert wird. Solange diese Systeme vor allem aus der Perspektive technischer Effizienz und gewinnorientierter Plattformlogik gedacht werden, bleiben die Erfahrungen der Betroffenen – insbesondere mehrfach-diskriminierter Personen und Gruppen – unsichtbar.
Ein feministischer Ansatz bedeutet deshalb mehr als nur „bessere Moderation“: Er fordert, dass Plattformen ihre Verantwortung anerkennen, intersektionale Risiken ernst nehmen und Meldewege so gestalten, dass sie Schutz, Handlungssouveränität und Gerechtigkeit schaffen.
Dazu gehört, Gewalt im sozialen Nahraum nicht auszublenden, sondern als zentralen Teil geschlechtsspezifischer Gewalt mitzudenken.
Wenn Plattformen in der Europäischen Union sichere digitale Räume schaffen wollen, führt kein Weg an feministischer, intersektionaler und betroffenenorientierter Gestaltung vorbei. Diese Empfehlungen zeigen auf, wie das aussehen kann – und wo die Plattformen dringend nachbessern müssen.

Ansprechpartnerin:

Elizabeth Ávila González
digitalegewalt@bv-bff.de

Glossar

Außergerichtliche Streitbeilegungsstellen

Wenn eine Plattform einen Post oder Account löscht oder eine Beschwerde ignoriert, können Nutzer*innen sich an so eine Stelle wenden. Sie prüft unabhängig, ob die Entscheidung der Plattform rechtmäßig war - ohne dass man direkt vor Gericht gehen muss.

Click fatigue

Click fatigue beschreibt die Erschöpfung oder Abstumpfung von Nutzer*innen, die entsteht, wenn Plattformen sie mit zu vielen Meldungen, Auswahlfenstern, Zustimmungsabfragen oder Sicherheitswarnungen konfrontieren. Durch die Überlastung klicken Menschen oft genervt weiter - was die Wirksamkeit von Sicherheits- oder Schutzmechanismen untergräbt und manipulative Design begünstigen kann.

Deceptive Design (manipulative Oberflächengestaltung)

Deceptive Design (Dark Patterns) bezeichnet Gestaltungstricks in digitalen Oberflächen, die Nutzer*innen bewusst in Entscheidungen drängen, die sie sonst nicht treffen würden – etwa durch Irreführung, Manipulation oder das Verstecken von wichtigen Optionen. Ziel ist meist, Daten zu sammeln, Zustimmung zu erzwingen oder ökonomische Vorteile für die Plattform zu erzielen.

Deepfake

Deepfakes sind gefälschte digitale Darstellungen, meistens von Videos, die mithilfe von Software erstellt werden. Dabei werden Gesichter oder Stimmen von Personen in bestehende Aufnahmen eingefügt, um den Eindruck zu erwecken, dass sie etwas sagen oder tun, was in Wirklichkeit nicht der Fall ist. Diese Technologie wird häufig zur Erstellung von gefälschten pornografischen Inhalten verwendet.

Digitale geschlechtsspezifische Gewalt

Digitale Gewalt ist ein Sammelbegriff. Gemeint sind Gewalthandlungen, die mithilfe informationstechnischer Systeme begangen werden:

- Gewalt mit technischen Geräten (z.B. Smartphones, Standort-Trackern, Kameras)
- mit Software, (Apps, Internetanwendungen, Mails etc.)
- und Gewalt im digitalen Raum, z.B. auf Online-Portalen oder sozialen Plattformen.

Wichtig ist dabei unser Verständnis von digitaler Gewalt als Kontinuum zu analoger Gewalt: Digitale Mittel erweitern und verstärken bestehende Muster von Kontrolle, Überwachung, Einschüchterung oder Demütigung. Die Gewalt verändert nicht ihren Kern – sie digitalisiert sich lediglich.

Digital Services Act (DSA)

Das ist ein EU-Gesetz, das große Plattformen, wie Facebook oder TikTok verpflichtet, besser gegen digitale Gewalt oder Desinformation vorzugehen. Zum Beispiel müssen sie erklären, wie ihre Algorithmen funktionieren, und schnell reagieren, wenn Nutzer*innen illegale Inhalte melden.

Digital Services Coordinator (DSC)

Das ist die nationale Aufsichtsbehörde für den DSA – in Deutschland ist das die Bundesnetzagentur. Sie sorgt dafür, dass Plattformen sich an die Regeln halten und nimmt dementsprechend Beschwerden an. Sie kann Bußgelder verhängen oder mit anderen EU-Stellen zusammenarbeiten.

Doxing
Doxing ist das internetbasierte Zusammentragen persönlicher Daten und die anschließende Veröffentlichung dieser Daten mit dem Ziel, die Betroffene bloßzustellen und einzuschüchtern.

Engagement
Engagement beschreibt wie stark Nutzer*innen mit Inhalten auf einer Plattform interagieren. Dazu zählen beispielsweise Likes, Kommentare, Teilen, Speichern oder Anklicken. Plattformen werten Engagement aus, um zu entscheiden, welche Inhalte besonders sichtbar gemacht werden. Inhalte mit viel Engagement werden oft weiter verbreitet – auch dann, wenn sie problematisch oder gewaltvoll sind.

Intersektionalität nach Kimberlé Crenshaw
Intersection (eng) heißt so viel wie „(Straßen)kreuzung“, Schnittmenge“. Intersektionale Ansätze und Analysen berücksichtigen, dass verschiedene soziale Kategorien durch Machtverhältnisse bedingt sind und im Zusammenwirken und in ihren Wechselwirkungen Einfluss auf (strukturelle) Ungleichheiten haben. Für digitale Gewalt bedeutet dies zum Beispiel, dass Frauen online angegriffen werden, weil sie Frauen sind, aber auch weil sie Schwarze Frauen sind oder trans oder beeinträchtigt und of color. Es geht also nicht nur um Sexismus und geschlechtsspezifische Gewalt, sondern auch um andere Gewaltformen, wie Rassismen und Ableismus. Die Ebenen sind verschränkt und lassen sich nicht unbedingt trennen, tragen aber zu unterschiedlichen Diskriminierungserfahrungen bei.

Non-consensual intimate image (NCII)
Non-Consensual Intimate Images (NCII) bezeichnet die Verbreitung, Weitergabe oder Veröffentlichung intimer Bilder oder Videos einer Person ohne deren ausdrückliche Einwilligung. Dazu zählt auch das Androhen der Veröffentlichung. NCII ist eine Form digitalisierter geschlechtsspezifischer Gewalt und kann schwerwiegende persönliche, soziale und berufliche Folgen für Betroffene haben.

Nudify-Apps
Nudify-Apps sind Apps oder Programme, die mit Hilfe von sogenannter Künstlicher Intelligenz Bilder oder Videos von Menschen so verändern, dass es aussieht, als wären sie nackt. Die betroffenen Personen haben dem meist nicht zugestimmt. Die so verübte Gewalt wird überwiegend gegenüber weiblich gelesenen Personen in einer sexualisierten Art und Weise ausgeübt.

SPOC
Single Point of Contact (SPOC) nach Artikel 12 DSA ist eine zentrale, leicht erreichbare Kontaktstelle einer Plattform, über die Nutzer*innen Kontakt aufnehmen können oder Rückfragen stellen können. Der SPOC soll sicherstellen, dass Plattformen überhaupt ansprechbar sind, insbesondere bei rechtswidrigen oder gewaltvollen Inhalten.

Stalkerware
Stalkerware bezeichnet Spionage-Apps oder -Programme, die heimlich auf Geräten installiert werden, um eine Person auszuspähen – etwa ihre Nachrichten, Standorte, Fotos oder Online-Aktivitäten. Die Nutzung von Stalkerware ist eine Form digitaler Gewalt und wird häufig in Kontexten von Partnerschaftsgewalt eingesetzt, um Kontrolle und Überwachung auszuüben.

Risk Reports
Risk Reports nach Artikel 34 DSA sind verpflichtende Risikoanalysen, die sehr große Online-Plattformen und Suchmaschinen regelmäßig durchführen und veröffentlichen müssen. Darin müssen sie systemische Risiken identifizieren – etwa

die Förderung von geschlechtsspezifischer Gewalt, Diskriminierung oder die Verbreitung illegaler Inhalte – sowie erklären, wie diese Risiken entstehen und welche Auswirkungen sie haben. Die Berichte bilden die Grundlage dafür, geeignete Schutz- und Minderungsmaßnahmen zu entwickeln.

Trusted Flagger (Vertrauenswürdige Hinweisgeber*innen)
Das sind Organisationen oder Stellen, die Plattformen besonders vertrauen. Sie können schneller und mit höherer Priorität Inhalte melden, die gegen das Gesetz verstoßen. Ihre Meldungen müssen von den Plattformen bevorzugt geprüft werden.

VLOPs/VLOSEs
Das sind sehr große Online-Plattformen (Very Large Online Platforms / VLOPs) oder sehr große Online-Suchmaschinen (Very Large Online Search Engines / VLOSEs), wie zum Beispiel Instagram, TikTok oder Google. Sie haben besonders viele Nutzer*innen in der EU – mindestens 45 Millionen. Für sie gelten deshalb strengere Regeln nach dem Digital Services Act. Eine Auflistung der VLOPs/VLOSes finden Sie **HIER**.

Impressum

Projekt „Aktiv gegen digitale Gewalt“
des Bundesverband Frauenberatungsstellen und Frauennotrufe (bff), Berlin

digitalegewalt@bv-bff.de

www.aktiv-gegen-digitale-gewalt.de

bff:
Bundesverband
Frauenberatungsstellen
und Frauennotrufe